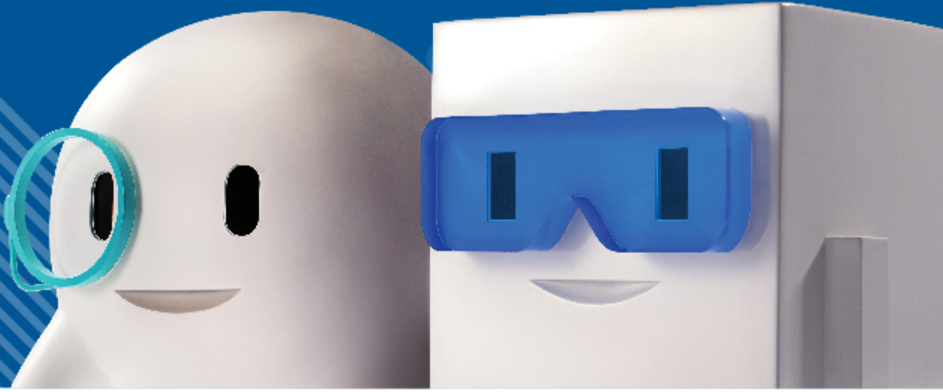
HKCERT
www.hkcert.org

HKPC

Reinforcing Security Protection for Websites



Wally Wong MA, CISSP
Security Analyst
HKCERT

All-round Productivity Partner
全方位企業伙伴

Motives of hacking your website

Your website has...	Criminals can get...
Powerful CPU and bandwidth (you got a server!)	Use your power → DDoS attack others
24 x 7 service	24 x 7 phishing/malware hosted in your site
Visitors	Put malware in your site to infect your visitors

Business impacts of hacked website

- Blacklist → interrupt your communication
  - Examples: Google, anti-virus, firewall, mail server
- Reputation → trust of your products/services
- Possible regulatory/legal consequences
  - Authority investigation (e.g. PCPD)
  - Law enforcement investigation
  - Class action lawsuit

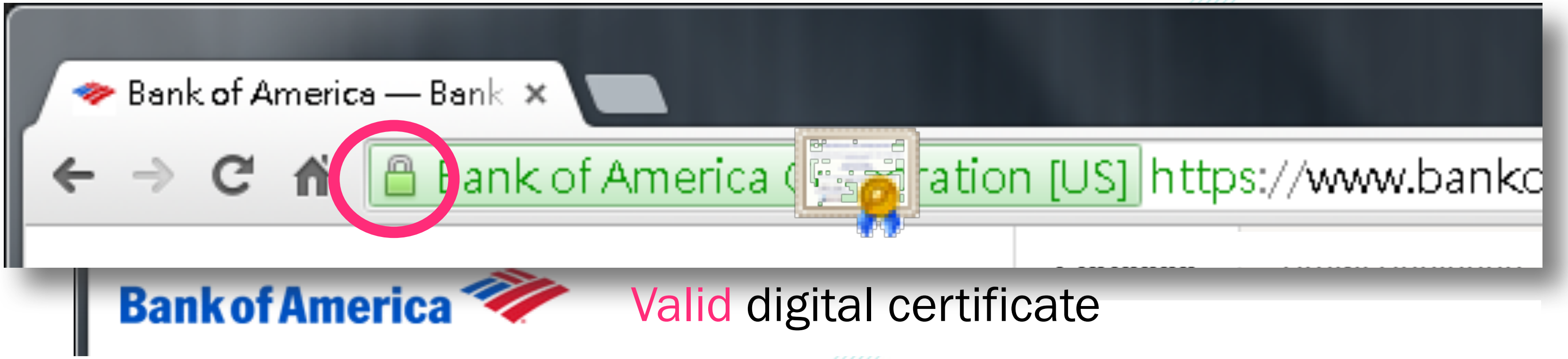
Secure website?

- Secure HTTP connection (HTTPS)
  Between you and your clients
- Secure web server
  Secure web application
  Your facilities

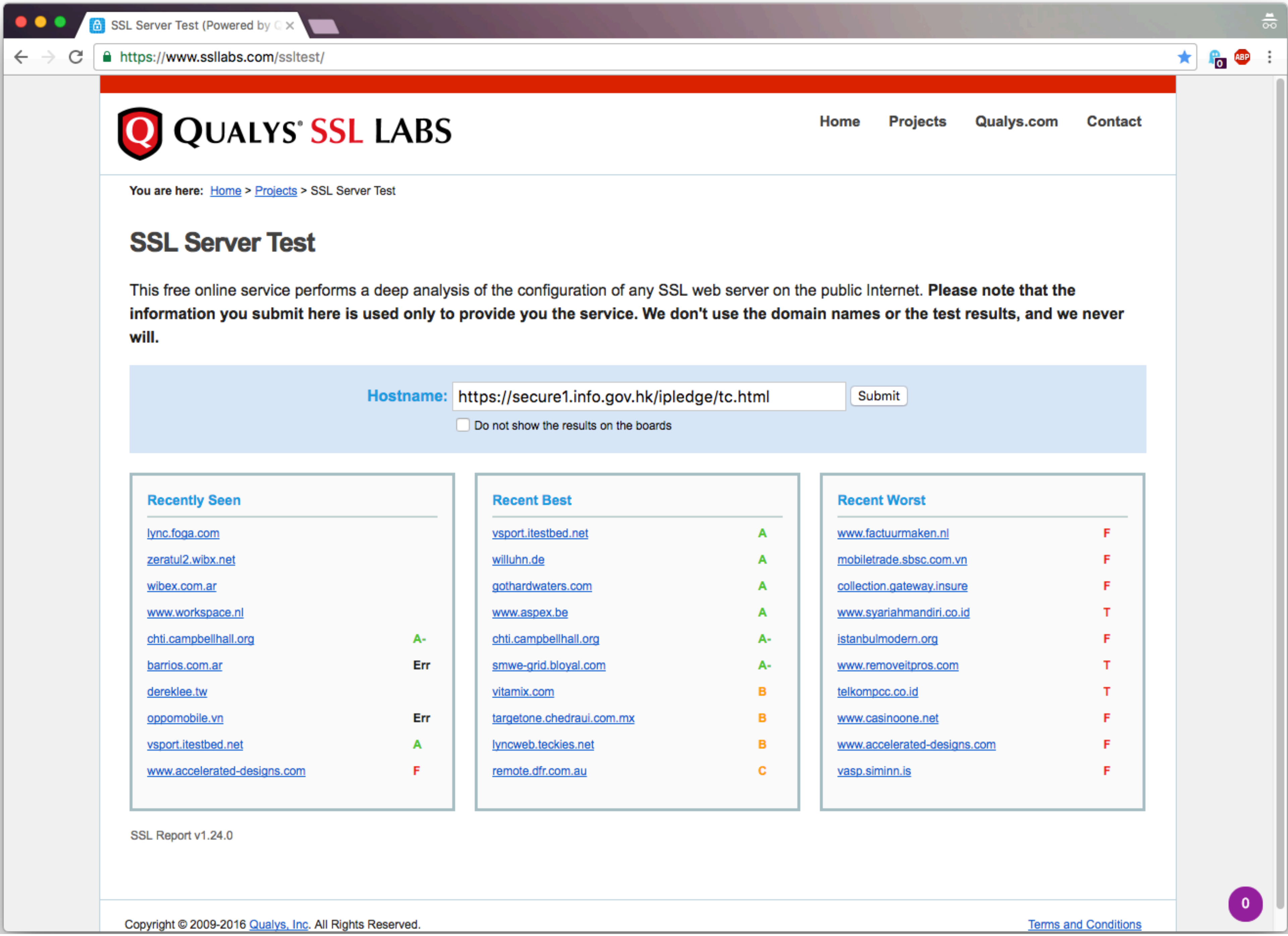
Secure HTTP connection

→ SSL or HTTPS (安全通訊協定) is ‘secure’

encrypt your data + AUTHENTIC WEBSITE BY THAT COMPANY



Valid digital certificate



SSL Server Test (Powered by Q
https://www.ssllabs.com/ssltest/
QUALYS® SSL LABS
Home
Projects
Qualys.com
Contact

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: https://secure1.info.gov.hk/ipledge/tc.html Submit

□ Do not show the results on the boards

Recently Seen	
lync.foga.com	
zeratul2.wibx.net	
wibex.com.ar	
www.workspace.nl	
chti.campbellhall.org	A-
barrios.com.ar	Err
dereklee.tw	
oppomobile.vn	Err
vsport.itestbed.net	A
www.accelerated-designs.com	F

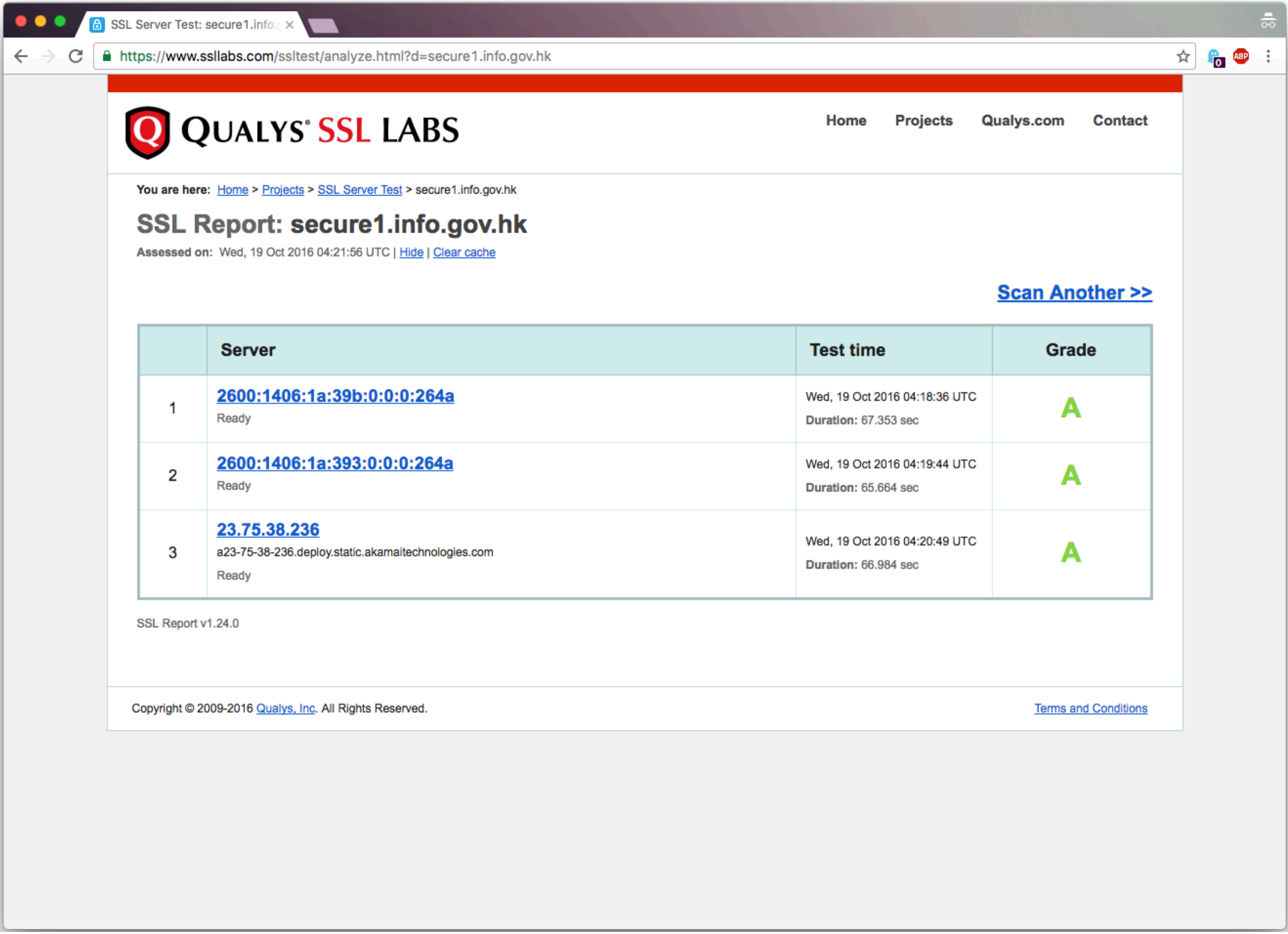
Recent Best	
vsport.itestbed.net	A
willuhn.de	A
gothardwaters.com	A
www.aspex.be	A
chti.campbellhall.org	A-
smwe-grid.bloyal.com	A-
vitamix.com	B
targetone.chedraui.com.mx	B
lyncweb.teckies.net	B
remote.dfr.com.au	C

Recent Worst	
www.factuurmaken.nl	F
mobiletrade.sbsc.com.vn	F
collection.gateway.insure	F
www.syariahmandiri.co.id	T
istanbulmodern.org	F
www.removeitpros.com	T
telkompcc.co.id	T
www.casinoone.net	F
www.accelerated-designs.com	F
vasp.siminn.is	F

SSL Report v1.24.0

Copyright © 2009-2016 Qualys, Inc. All Rights Reserved.

Terms and Conditions



SSL Server Test: secure1.info.
https://www.ssllabs.com/ssltest/analyze.html?d=secure1.info.gov.hk
QUALYS SSL LABS
Home
Projects
Qualys.com
Contact

You are here: Home > Projects > SSL Server Test > secure1.info.gov.hk

SSL Report: secure1.info.gov.hk

Assessed on: Wed, 19 Oct 2016 04:21:56 UTC | Hide | Clear cache

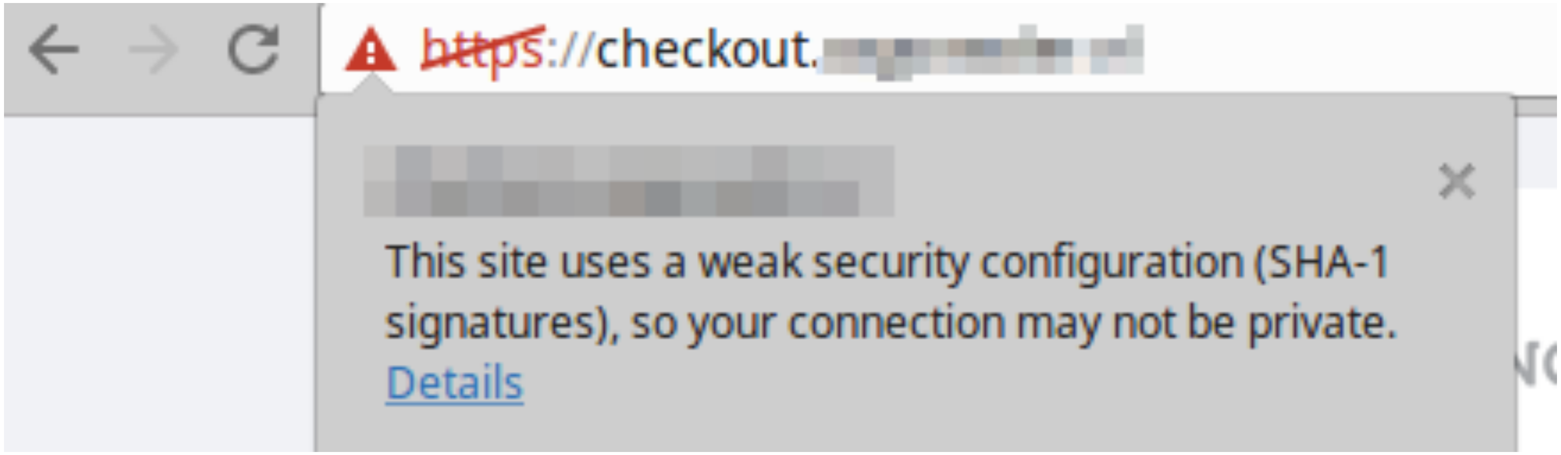
Scan Another >>

	Server	Test time	Grade
1	2600:1406:1a:39b:0:0:0:264a Ready	Wed, 19 Oct 2016 04:18:36 UTC Duration: 67.353 sec	A
2	2600:1406:1a:393:0:0:0:264a Ready	Wed, 19 Oct 2016 04:19:44 UTC Duration: 65.664 sec	A
3	23.75.38.236 a23-75-38-236.deploy.static.akamaitechnologies.com Ready	Wed, 19 Oct 2016 04:20:49 UTC Duration: 66.984 sec	A

SSL Report v1.24.0

Copyright © 2009-2016 Qualys, Inc. All Rights Reserved.

Terms and Conditions

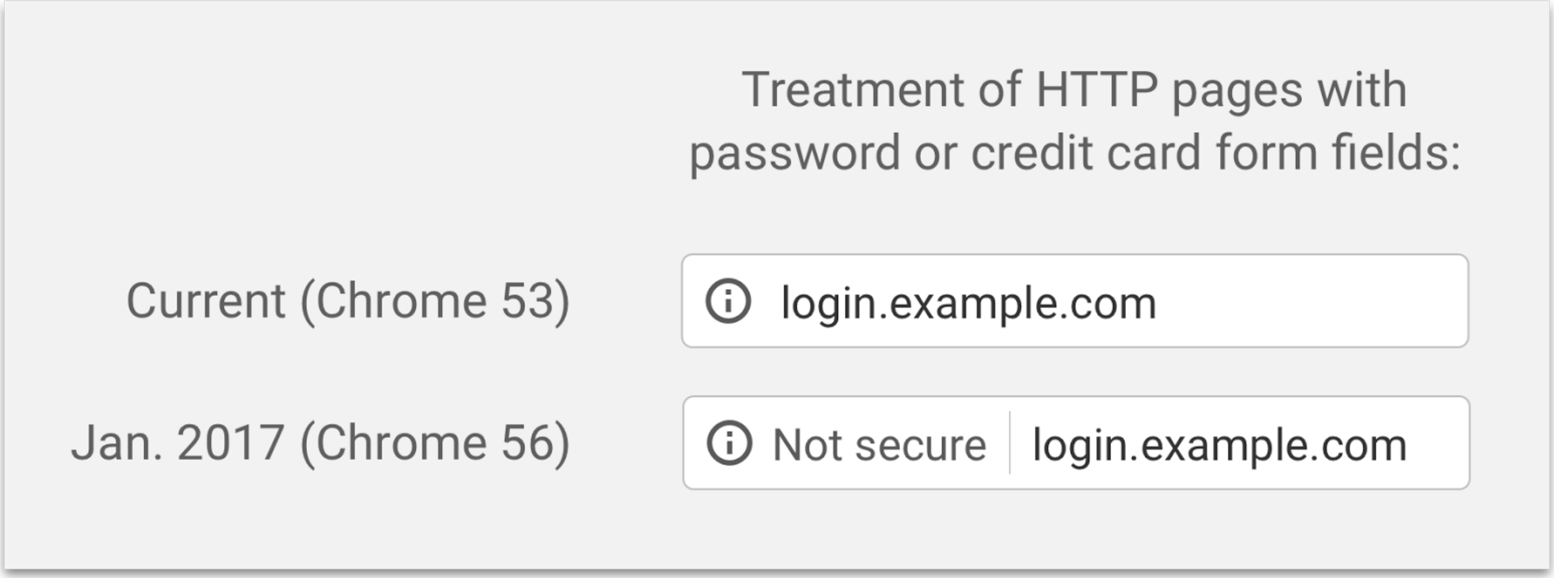


~~https~~://checkout.[redacted]

[redacted]

This site uses a weak security configuration (SHA-1 signatures), so your connection may not be private. Details

https://gwillem.gitlab.io/assets/img/sha1.png



Treatment of HTTP pages with password or credit card form fields:

Current (Chrome 53)	ⓘ login.example.com
Jan. 2017 (Chrome 56)	ⓘ Not secure | login.example.com

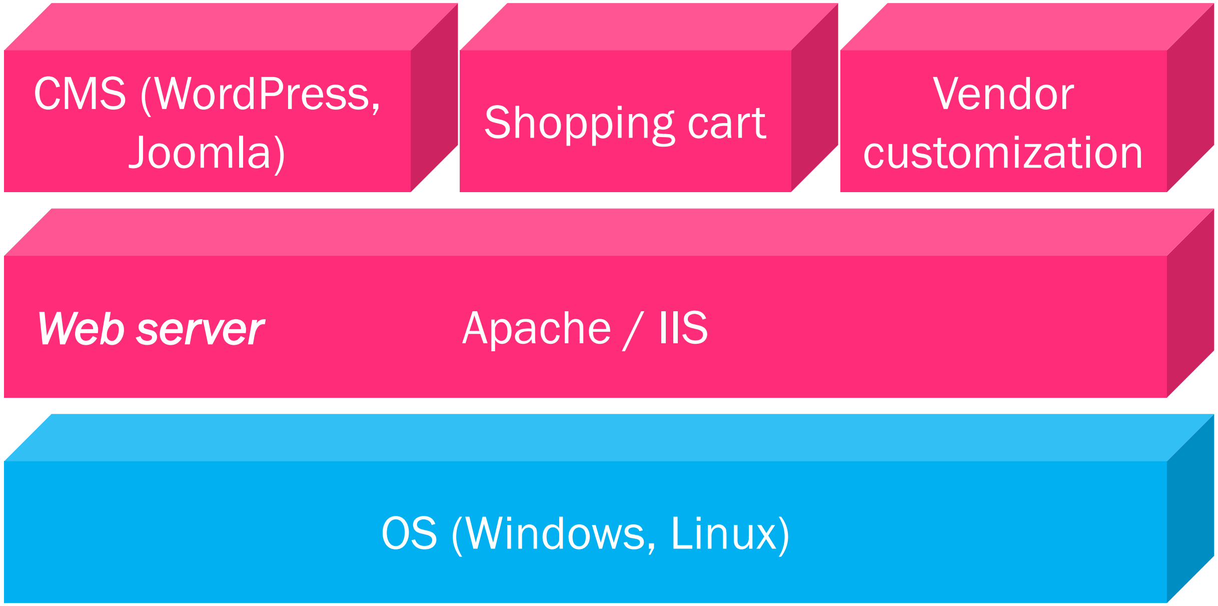
https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html

Secure website?

- Secure HTTP connection (HTTPS)
  Between you and your clients
- Secure web server (e.g. Apache, IIS)
  Secure web application (e.g. CMS, shopping cart)
  Your facilities

Vulnerability Scanning

- Misconfiguration / Vulnerability management
- Weak authentication / access control / encryption
- Weak input validation



CMS (WordPress, Joomla)

Shopping cart

Vendor customization

Web server

Apache / IIS

OS (Windows, Linux)

Ron Chan

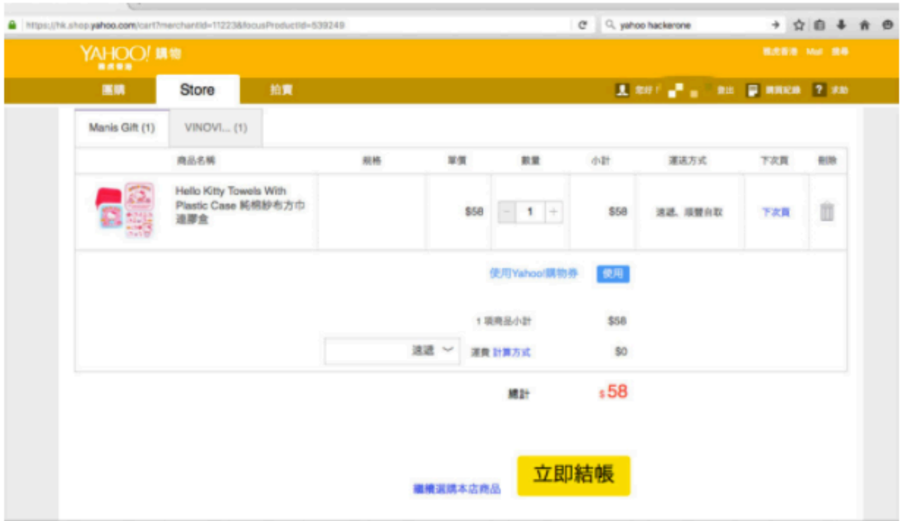
This is about cyber security

- About
- Contact

RECENT POSTS

Abusing Multistage Logic Flaw to Buy Anything for Free at hk.deals.yahoo.com

Yahoo! Deals, Shop, Auctions, are quite prmoinent service in Hong Kong, they provide a platform that allows user to trade items with Yahoo Payment system. I started to buy an item at hk.shop.yahoo.com, I followed along the process and monitor the traffic by Burp Suite.



https://hk.shop.yahoo.com/cart?merchantId=11223&focusProductId=539249
yahoo hackerone
YAHOO! 購物
團購
Store
拍賣
Manis Gift (1)
VINOVI... (1)

	商品名稱	規格	單價	數量	小計	運送方式	下次買	刪除
	Hello Kitty Towels With Plastic Case 純棉紗布方巾連膠盒		$58	1	$58	速遞、順豐自取	下次買	

使用Yahoo!購物券 使用

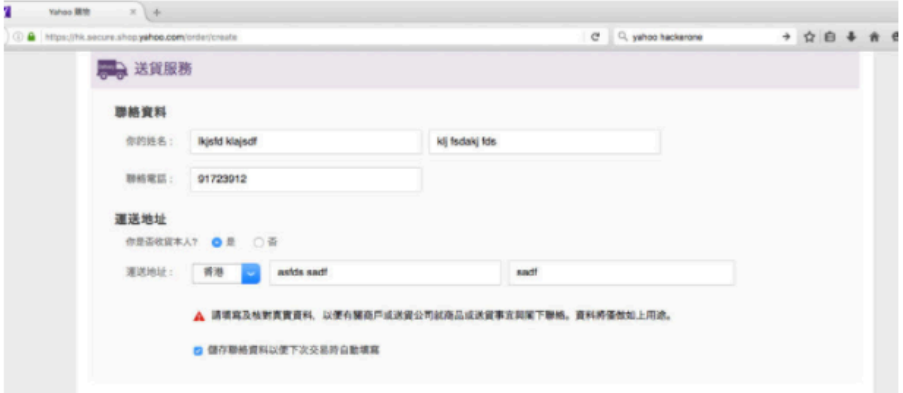
1 項商品小計 $58

速遞 運費 計算方式 $0

總計 $58

繼續選購本店商品 立即結帳

Buying Page in Yahoo



送貨服務

聯絡資料

你的姓名： ikjsfd klajsdf　klj fsdakj fds

聯絡電話： 91723912

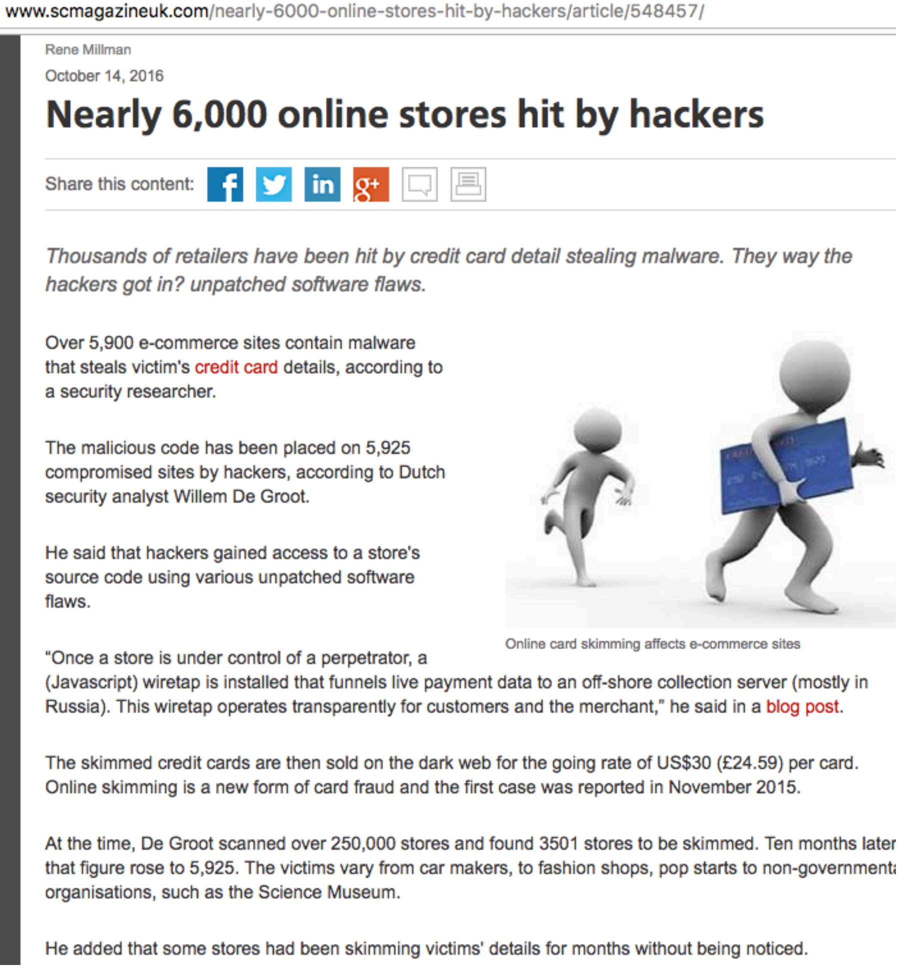
運送地址

你是否收貨本人? ● 是 ○ 否

運送地址： 香港　asfds sadf　sadf

請填寫及核對真實資料，以便有關商戶或送貨公司就商品或送貨事宜與閣下聯絡。資料將僅做如上用途。

☑ 儲存聯絡資料以便下次交易時自動填寫



www.scmagazineuk.com/nearly-6000-online-stores-hit-by-hackers/article/548457/

Rene Millman

October 14, 2016

Nearly 6,000 online stores hit by hackers

Share this content:

Thousands of retailers have been hit by credit card detail stealing malware. They way the hackers got in? unpatched software flaws.

Over 5,900 e-commerce sites contain malware that steals victim's credit card details, according to a security researcher.

The malicious code has been placed on 5,925 compromised sites by hackers, according to Dutch security analyst Willem De Groot.

He said that hackers gained access to a store's source code using various unpatched software flaws.

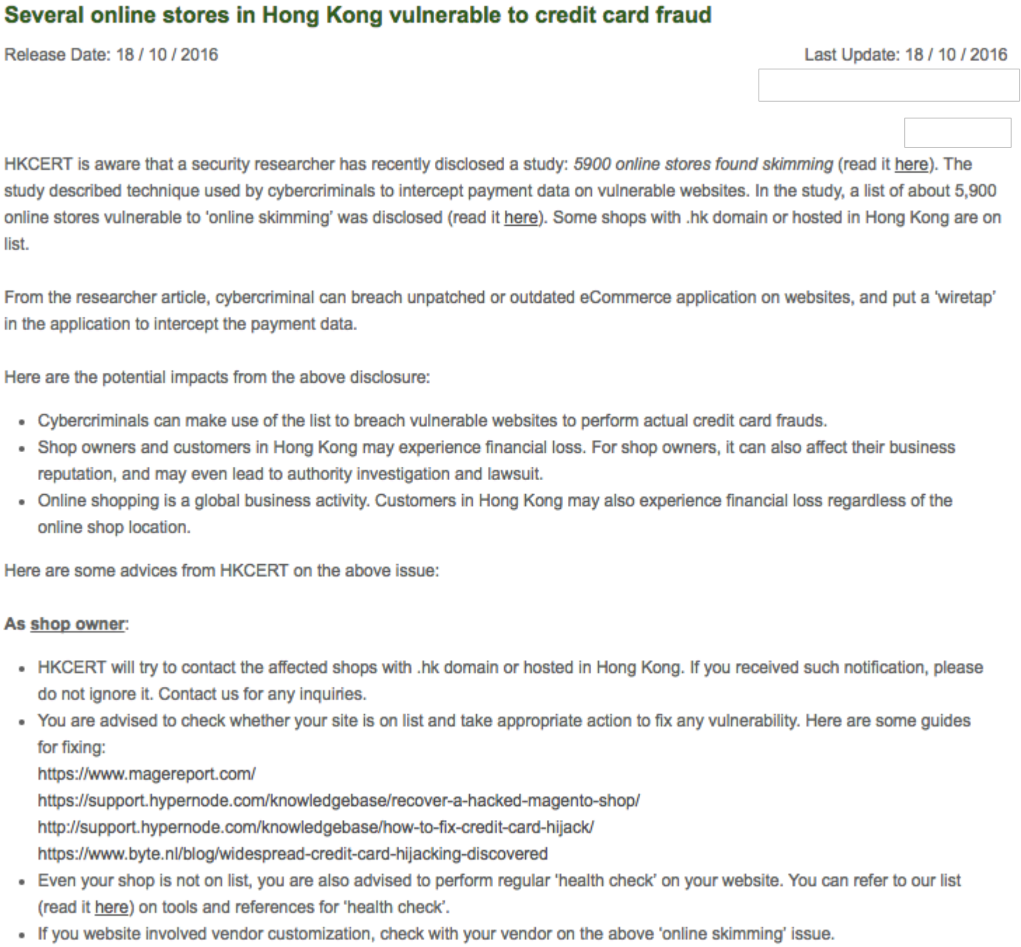
Online card skimming affects e-commerce sites

"Once a store is under control of a perpetrator, a (Javascript) wiretap is installed that funnels live payment data to an off-shore collection server (mostly in Russia). This wiretap operates transparently for customers and the merchant," he said in a blog post.

The skimmed credit cards are then sold on the dark web for the going rate of US$30 (£24.59) per card. Online skimming is a new form of card fraud and the first case was reported in November 2015.

At the time, De Groot scanned over 250,000 stores and found 3501 stores to be skimmed. Ten months later that figure rose to 5,925. The victims vary from car makers, to fashion shops, pop starts to non-governmenta organisations, such as the Science Museum.

He added that some stores had been skimming victims' details for months without being noticed.



Several online stores in Hong Kong vulnerable to credit card fraud

Release Date: 18 / 10 / 2016

Last Update: 18 / 10 / 2016

HKCERT is aware that a security researcher has recently disclosed a study: *5900 online stores found skimming* (read it here). The study described technique used by cybercriminals to intercept payment data on vulnerable websites. In the study, a list of about 5,900 online stores vulnerable to 'online skimming' was disclosed (read it here). Some shops with .hk domain or hosted in Hong Kong are on list.

From the researcher article, cybercriminal can breach unpatched or outdated eCommerce application on websites, and put a 'wiretap' in the application to intercept the payment data.

Here are the potential impacts from the above disclosure:

- Cybercriminals can make use of the list to breach vulnerable websites to perform actual credit card frauds.
- Shop owners and customers in Hong Kong may experience financial loss. For shop owners, it can also affect their business reputation, and may even lead to authority investigation and lawsuit.
- Online shopping is a global business activity. Customers in Hong Kong may also experience financial loss regardless of the online shop location.

Here are some advices from HKCERT on the above issue:

As shop owner:

- HKCERT will try to contact the affected shops with .hk domain or hosted in Hong Kong. If you received such notification, please do not ignore it. Contact us for any inquiries.
- You are advised to check whether your site is on list and take appropriate action to fix any vulnerability. Here are some guides for fixing:
  https://www.magereport.com/
  https://support.hypernode.com/knowledgebase/recover-a-hacked-magento-shop/
  http://support.hypernode.com/knowledgebase/how-to-fix-credit-card-hijack/
  https://www.byte.nl/blog/widespread-credit-card-hijacking-discovered
- Even your shop is not on list, you are also advised to perform regular 'health check' on your website. You can refer to our list (read it here) on tools and references for 'health check'.
- If you website involved vendor customization, check with your vendor on the above 'online skimming' issue.

Hack your website

- ‘Vulnerable website’ can mean:
  - web server (e.g. Linux + Apache, Windows + IIS), or/and
  - web app (e.g. Joomla, WordPress) is/are vulnerable
- Reasons for web server/app vulnerable:
  - No regular patch/update.
  - Outdated version.
  - Use vulnerable plugins.
  - Misconfiguration (e.g. too much privilege)
  - Web form input (e.g. contact us) implemented by developer/vendor → not enough input validation

SME Free Web Security Health Check Pilot Scheme

- Promote the best practice of “Check-Act-Verify” approach for website security health check to SME.
- Prerequisites:
  - You must has a website!
  - Willing to allocate resources for follow-up.
  - Apply: submit documents, arrange schedule

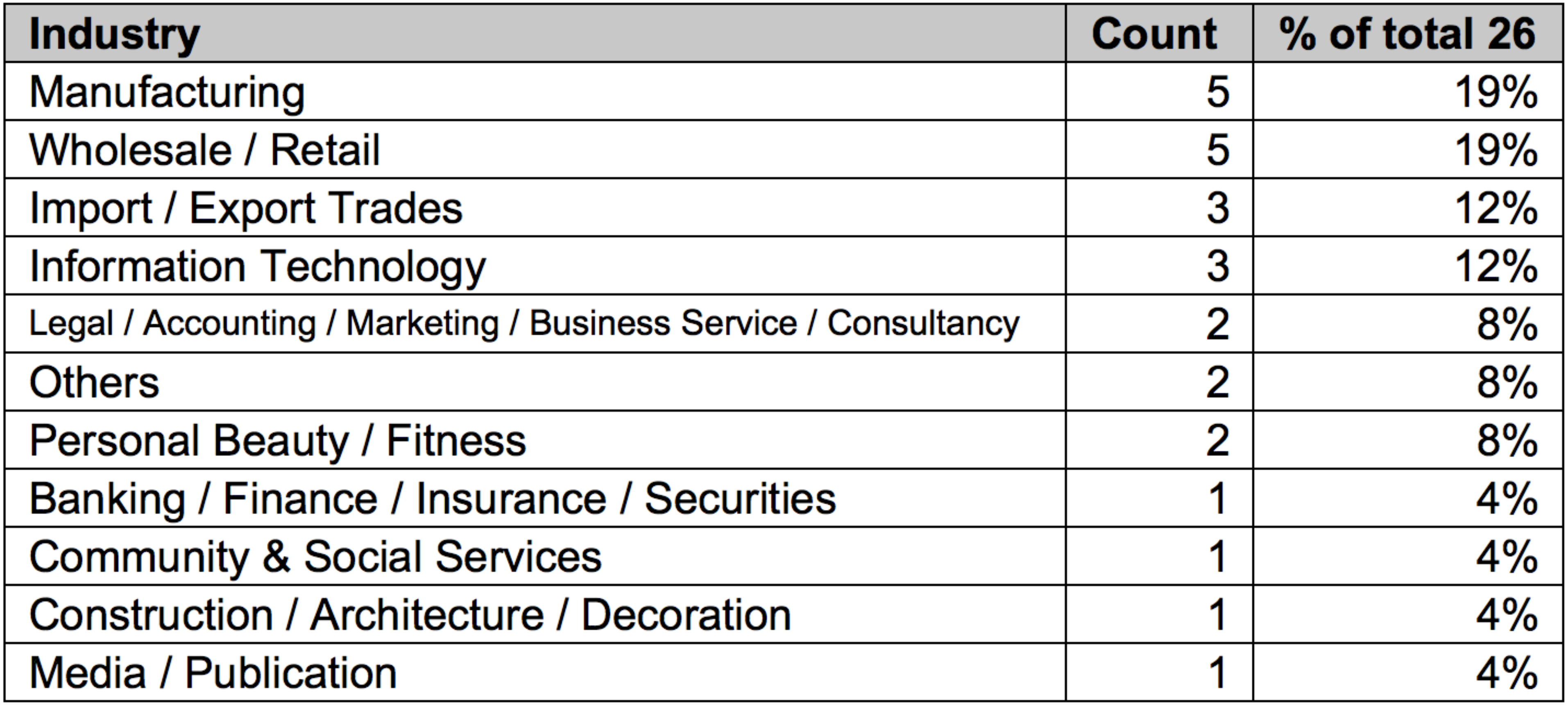
Friends of SME One
中小企業網站免費保安檢查先導計劃

「網站」是企業推廣服務、客戶關係管理和網上交易服務的重要工具。然而，部分企業，尤其是中小企業(SMEs)，沒有足夠的資源去確保網站的安全。有見及此，SME One誠意為Friends of SME One提供「中小企業網站免費保安檢查先導計劃」，在專家指導下為中小企業的網站進行「檢查-行動-驗證」。計劃是免費的，並由香港生產力促進局轄下的香港電腦保安事故協調中心（HKCERT）舉辦，旨在向中小企業推廣網站保安的最佳實踐方法。

SME Free Web Security Health Check Pilot Scheme

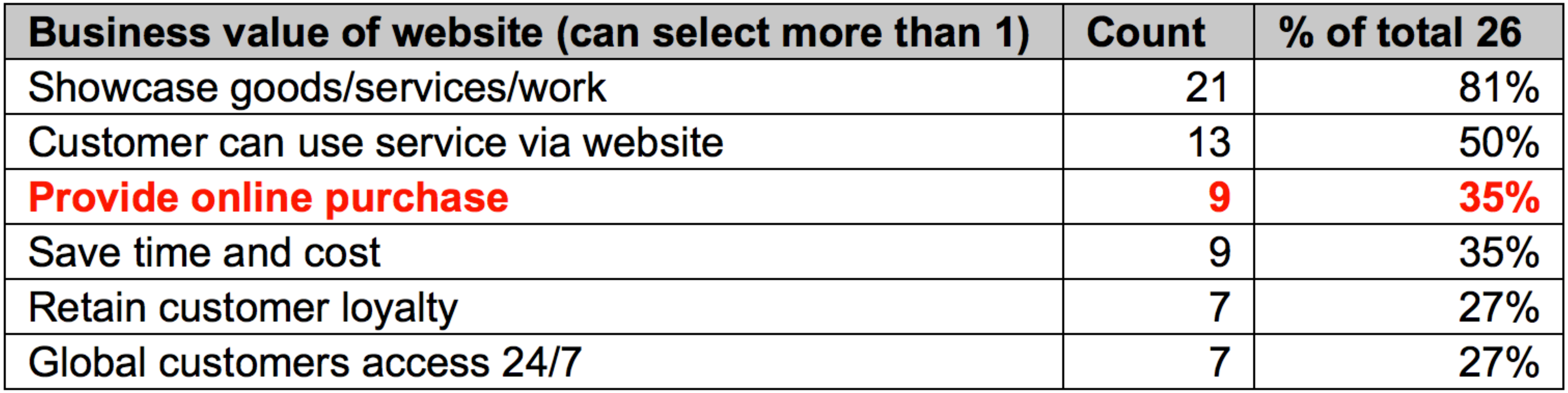
- 35 companies joined, 30 completed health check
- First and second round of scanning completed, with scan results presented in report:
    - Website vulnerability severity levels
    - Classify vulnerabilities into 6 types
    - Business impacts
    - Titles of vulnerabilities found
    - Remediation advice for technical staff to fix problems
- Final report on overall result will be published.

Distribution of Industry in Participants



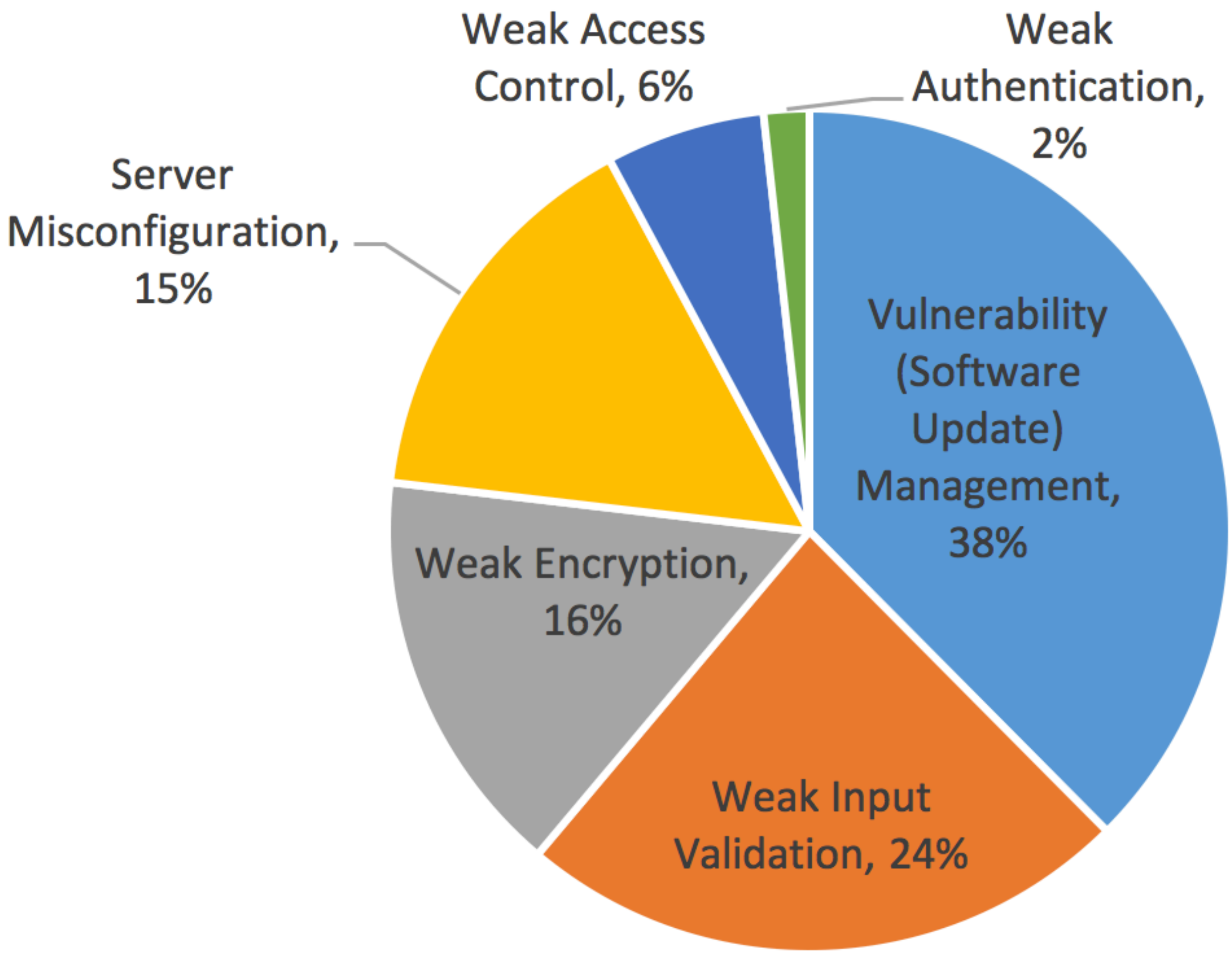
Industry	Count	% of total 26
Manufacturing	5	19%
Wholesale / Retail	5	19%
Import / Export Trades	3	12%
Information Technology	3	12%
Legal / Accounting / Marketing / Business Service / Consultancy	2	8%
Others	2	8%
Personal Beauty / Fitness	2	8%
Banking / Finance / Insurance / Securities	1	4%
Community & Social Services	1	4%
Construction / Architecture / Decoration	1	4%
Media / Publication	1	4%

Business Values of Your Website

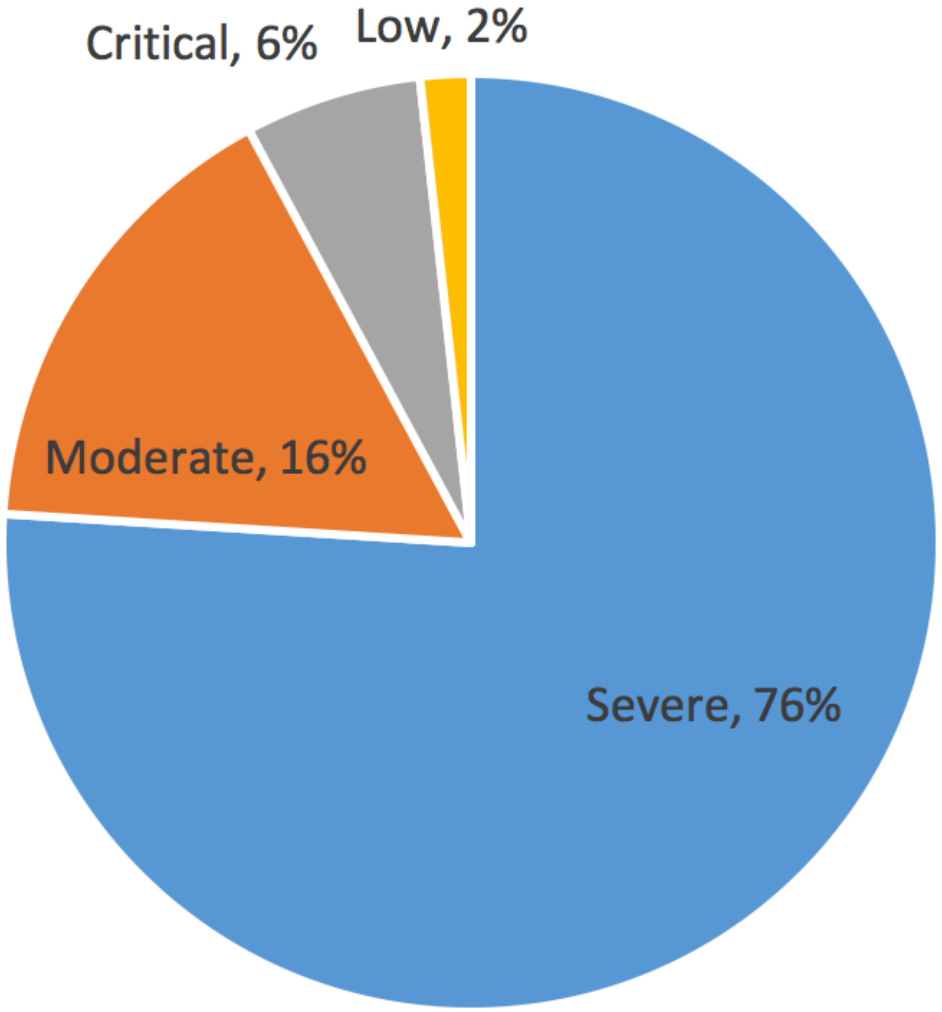


Business value of website (can select more than 1)	**Count**	**% of total 26**
Showcase goods/services/work	21	81%
Customer can use service via website	13	50%
Provide online purchase	**9**	**35%**
Save time and cost	9	35%
Retain customer loyalty	7	27%
Global customers access 24/7	7	27%

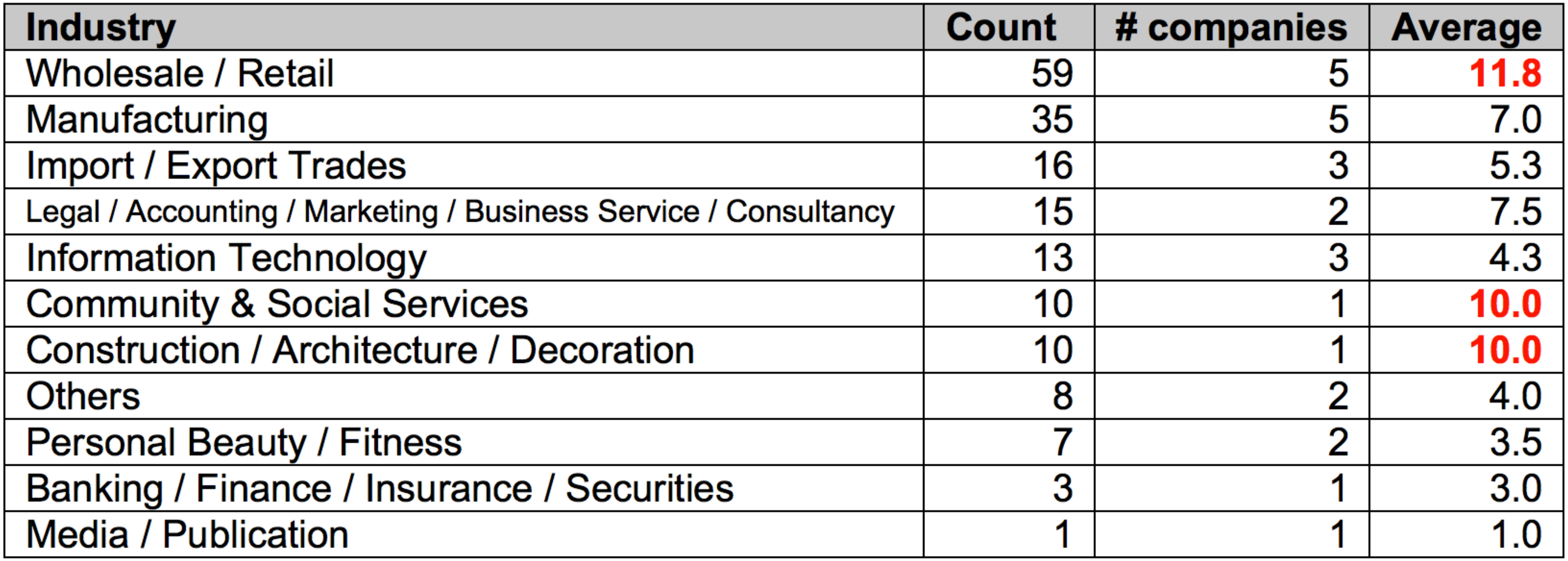
Distribution of Vulnerability Classification



Distribution of Vulnerability Severity Levels

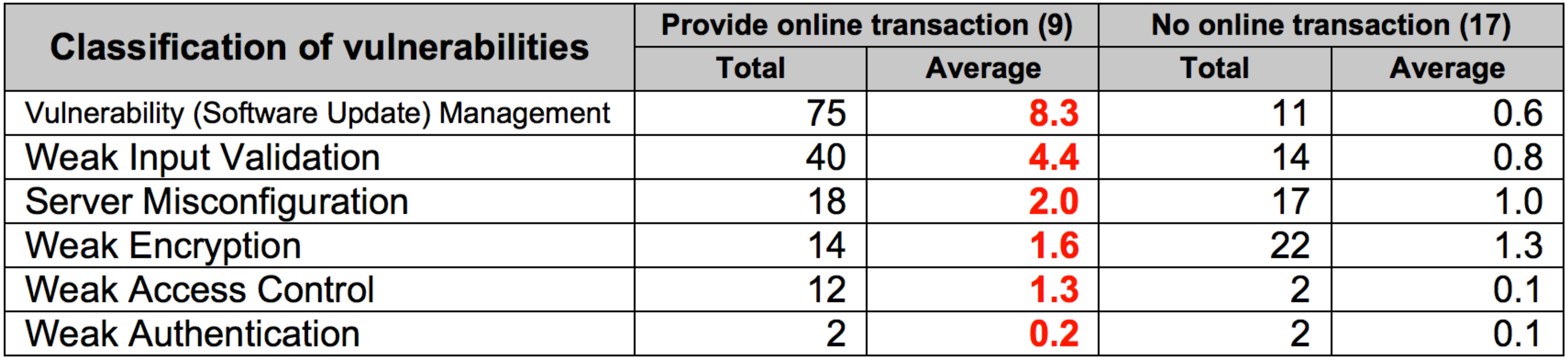


Industry vs Number of Vulnerabilities



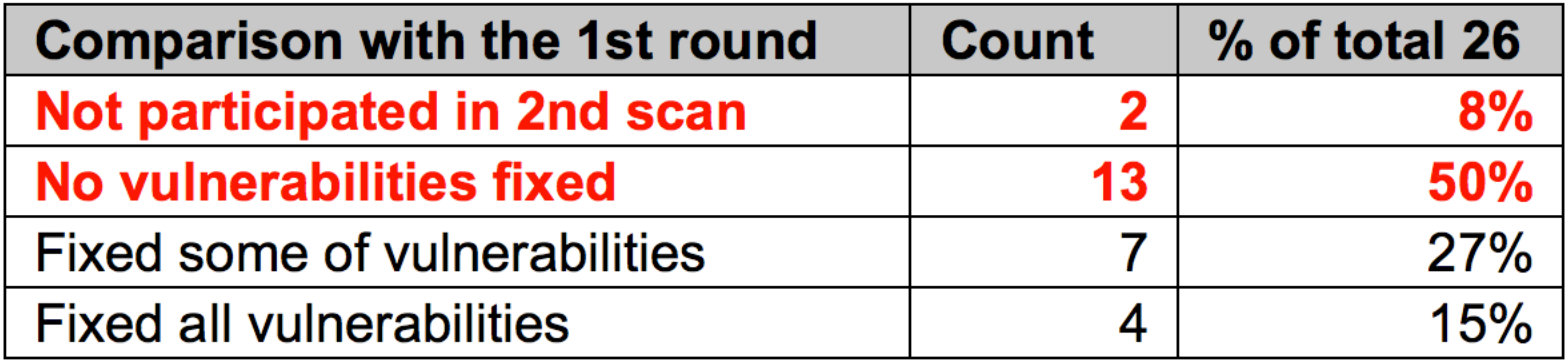
Industry	Count	# companies	Average
Wholesale / Retail	59	5	11.8
Manufacturing	35	5	7.0
Import / Export Trades	16	3	5.3
Legal / Accounting / Marketing / Business Service / Consultancy	15	2	7.5
Information Technology	13	3	4.3
Community & Social Services	10	1	10.0
Construction / Architecture / Decoration	10	1	10.0
Others	8	2	4.0
Personal Beauty / Fitness	7	2	3.5
Banking / Finance / Insurance / Securities	3	1	3.0
Media / Publication	1	1	1.0

Online Transaction vs Vulnerabilities



Classification of vulnerabilities	Provide online transaction (9)		No online transaction (17)	
	Total	Average	Total	Average
Vulnerability (Software Update) Management	75	8.3	11	0.6
Weak Input Validation	40	4.4	14	0.8
Server Misconfiguration	18	2.0	17	1.0
Weak Encryption	14	1.6	22	1.3
Weak Access Control	12	1.3	2	0.1
Weak Authentication	2	0.2	2	0.1

Comparison with the 1st scanning



Comparison with the 1st round	Count	% of total 26
Not participated in 2nd scan	2	8%
No vulnerabilities fixed	13	50%
Fixed some of vulnerabilities	7	27%
Fixed all vulnerabilities	4	15%

Improve and maintain security

- Assessment:
  - Scan website regularly, and follow up with the advice.
  - Assessed by credited criteria, e.g. OWASP Top 10, PCI DSS.
- Infrastructure:
  - Check that hosting company guaranteed secure features, e.g. regular patch, secure WordPress/Joomla, shopping cart etc.
  - Web application firewall (not to confuse with network firewall)
  - Consider cloud services.
- Detection:
  - Google Webmasters tools (developers.google.com/webmasters/hacked)
  - Check blacklist yourself, e.g. mxtoolbox.com/blacklists.aspx

Improve and maintain security

- User
  - Security protection of user workstations and devices (also at home).
- Website
  - Regular patch, update, vulerability scanning of web app/server.
  - Web app specific (e.g. CMS, eCommerce) security checking.
  - Regular offline backup.
- Prepare for emergency
  - Business contingency plan.
  - Drill for website down/breached.
  - Provide reachable contact on website/WHOIS so that organizations like HKCERT can contact you if your site was found hacked.
- If your website does not function any more, remove it completely (note: you may need to keep the domain).